AO 91 (Rev. 11/11) Criminal Complaint (Rev. by USAO on 3/12/20) ☐ Original ☐ Duplicate Original

UNITED STATES DISTRICT COURT

for the

Central District of California

United States of America

v.

Marian Iulian Sandu and Lucian Ionut Nechita,

Defendant(s).

Case No. 2:24-mj-00605-DUTY

CRIMINAL COMPLAINT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about February 2, 2024, in the county of Los Angeles in the Central District of California, the defendant violated:

Code Section	*Offense Description*
18 U.S.C. § 1029(a)(2)	Use of unauthorized access devices

This criminal complaint is based on these facts:

Please see attached affidavit.

☒ Continued on the attached sheet.

/s/
Complainant's signature

Adam Chang, Senior Investigator
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone.

Date: 2/2/2024

Judge's signature

City and state: Los Angeles, California

Hon. Jacqueline Chooljian, U.S. Magistrate Judge
Printed name and title

AUSA: Joseph De Leon (x7280)

AFFIDAVIT

I, Adam Chang, being duly sworn, declare and state as follows:

I. PURPOSE OF AFFIDAVIT

1. This affidavit is made in support of a criminal complaint against Marian Iulian Sandu ("SANDU") and Lucian Ionut NECHITA ("NECHITA"), who gave the alias of "Julio Zamora" for a violation of 18 U.S.C. § 1029(a)(2) (use of unauthorized access devices).

2. This affidavit is also made in support of an application for a warrant to search the following digital devices in the custody of the United States Secret Service ("USSS"), in Los Angeles, California, as described in Attachment A:

a. a Samsung cell phone retrieved from SANDU's person ("SUBJECT DEVICE 1"); and

b. an Apple iPhone XR retrieved from NECHITA's person ("SUBJECT DEVICE 2" and, collectively with SUBJECT DEVICE 1, the "SUBJECT DEVICES").

3. The requested search warrant seeks authorization to seize evidence, fruits, or instrumentalities of violations of 18 U.S.C. §§ 371 (Conspiracy), 1028 (Fraud and Related Activity in Connection with Identification Documents, Authentication Features, and Information), 1029 (Fraud and Related Activity in Connection with Access Devices), 1344 (Bank Fraud), and 1028A (Aggravated Identity Theft) (collectively, the "Subject Offenses"), as described more fully in Attachment B.

4. Attachments A and B are incorporated herein by reference.

5. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested complaint and search warrant, and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

II. BACKGROUND OF AFFIANT

6. I have been a peace officer in the State of California for approximately 15 years. I have been an Investigator for the Los Angeles County District Attorney's Office for the past six years. Before that, I was a Police Officer and later Detective for the Burbank Police Department. I currently hold an Advanced Peace Officer Standards and Training (POST) Certificate and a Certificate of Completion from the Robert Presley Institute of Criminal Investigation with a Specialty in Cybercrime Investigations. I have a Bachelor's Degree in Political Science/International Relations and a Master's Degree in Criminal Justice.

7. I graduated from the Los Angeles County Sheriff's Department Academy in 2008, where I received basic training as a peace officer. Since that time, I have received numerous

additional trainings, on both internet and electronic crimes and identity theft. I have completed the United States Secret Service National Computer Forensics Institute's (NCFI) Basic Network Investigation Training (BNIT), Basic Investigation of Computer and Electronic Crimes Program (BICEP), and Network Intrusion Response Program (NITRO). I have also served as proctor at NCFI in their Cyber Investigative Techniques (CIT) course. I am a CompTIA A+ Certified Professional.

8. I have been the Investigating Officer and affiant on numerous search warrants dealing with electronic crimes, ranging from fraud, identity theft, network intrusions, to child sexual abuse material investigations. Additionally, I have previously served as an affiant for several search warrants for the seizure of digital evidence from electronic communications providers, such as Google, Charter Communications, Facebook, and Verizon in cyber crime, identity theft, and child sexual abuse material investigations. Furthermore, I have recovered digital devices, such as computers, phones, and key loggers that were used to commit computer crimes. Evidence obtained from those search warrants have resulted in the identification of suspects and yielded critical evidence needed for criminal filing and convictions.

9. I am currently assigned to the United States Secret Service Cyber Fraud Task Force and the Los Angeles District Attorney's Cyber Investigation Response Team where we are primarily tasked with investigating electronic crimes, to include fraud, network intrusions, identity theft and online

child sexual abuse material. In this capacity, I am currently deputized as a Special Deputy United States Marshal.

III. SUMMARY OF PROBABLE CAUSE

10. Between August 2022 and January 2024, the California Department of Social Services ("DSS") has detected more than $100 million in stolen funds from victim Electronic Benefit Transfer ("EBT") cards. Much of this fraud is from two specific programs known as CalFresh and CalWORKs, which help low-income households pay for housing, food, and other necessary expenses. Many of the fraudulent withdrawals are done at specific ATMs in the Central District of California.

11. On February 1, 2024, at 5:00 a.m.[1], law enforcement conducted physical surveillance at a US Bank ATM terminal located at 18200 Western Avenue, Gardena, which was identified by DSS as one of the top ATM locations for EBT fraud.

12. At 7:14 a.m., law enforcement observed NECHITA at the ATM terminal. Upon arriving at the ATM, NECHITA immediately placed something on the ATM surveillance camera, which appeared to have been done to conceal his actions and identity. NECHITA withdrew approximately $2,440 from the ATM in rapid succession using approximately four different access devices.

13. At 7:25 a.m., law enforcement observed SANDU at the walk-up ATM terminal. SANDU withdrew approximately $1,640 in cash from the ATM in rapid succession using approximately three different access devices and used two additional access devices

[1] Unless otherwise noted, all times are Pacific and are approximate.

to conduct balance inquires that were unsuccessful. At 7:30 a.m., SANDU left the ATM and walked toward a 2014 blue BMW Coupe with a license plate number 9FEY325 (the "Subject Vehicle"). Law enforcement identified themselves as police and attempted to detain SANDU, but he did not listen to law enforcement commands and instead walked quickly towards the entrance of a nearby liquor store where he attempted to hide something on the counter. Law enforcement detained SANDU and found five access devices (later determined to be cloned cards encoded with the same EBT card information SANDU used to access victim accounts at the ATM) hidden on the counter. SANDU was arrested and found to be in possession of $1,640 in cash and of SUBJECT DEVICE 1.

14. At 7:30 a.m., law enforcement observed NECHITA standing next to the Subject Vehicle. As NECHITA was entering the Subject Vehicle, law enforcement identified themselves as police and detained NECHITA, who was carrying SUBJECT DEVICE 2. The Subject Vehicle contained 14 different access devices (later determined to be cloned cards) and $8,037.

IV. STATEMENT OF PROBABLE CAUSE

15. Based on my review of law enforcement reports, conversations with other law enforcement agents, and my own knowledge of the investigation, I am aware of the following:

A. Regulatory Background of CalFresh and CalWORKs Programs

16. DSS is a government agency that administers several benefit and assistance programs for residents of the State of California. One of the assistance programs administered by DSS

is called CalFresh (formerly known as food stamps), which helps low-income households purchase food and household items to meet their nutritional needs. Another assistance program administered by DSS is called CalWORKs, which helps low-income families with children pay for housing, food, and other necessary expenses.

17. Residents of California that meet the criteria established by the CalFresh or CalWORKs programs can apply online for benefits at www.getcalfresh.org and www.benefitscal.com. Beneficiaries apply for benefits by submitting their income and number of dependents to determine their benefit eligibility.

18. CalFresh and CalWORKs benefits are issued through Electronic Benefit Transfer cards ("EBT cards"). EBT cards are mailed to an address designated by the account holder and function like traditional debit cards to conduct transactions. For example, you can use an EBT card to make a purchase at a grocery or convenient store by swiping the card at a point-of-sale terminal.

19. The EBT cards issued under CalFresh and CalWORKs are assigned specific Bank Identification Numbers ("BIN"). A BIN refers to the first five digits of the account number on a debit or credit card and can be used to identify the issuer of the card, like DSS, which administers the CalFresh and CalWORKs programs.

20. Benefits received through the program are typically disbursed to EBT cardholders by DSS during the early days of

each month. Those benefits are deposited directly from DSS into the account of the EBT cardholder.

21. The EBT cardholders can then conduct cash withdrawals at automated teller machines ("ATMs") using a personal identification number ("PIN") established by the card holder. The EBT cardholder presents the card at an ATM, inserts the card into the ATM card reader, and utilizes a PIN to withdraw the funds previously deposited by DSS intended for beneficiaries of the CalFresh or CalWORKs programs.

A. Background on EBT Fraud in the Los Angeles Area and Prior State and Federal Operations

22. Since in or about August 2022, local law enforcement has been working with DSS to investigate a significant increase in unauthorized cash withdrawals utilizing EBT cards. Based on analysis of victim complaints to DSS, victim complaints to local law enforcement, bank records, and surveillance, law enforcement determined that the majority of the unauthorized cash withdrawals were being conducted with cloned cards.

23. A cloned card can be a blank white plastic card or another debit, credit or gift card that contains altered information on the card's magnetic stripe. Based on my training and experience, I know that suspects will often clone cards by taking stolen card information from a victim card's magnetic stripe and re-encode that stolen information onto another card's magnetic stripe. Cloning these cards allows the suspect to use the card and the DSS benefits added on to the account linked to the card for illicit purchases or unauthorized cash withdrawals.

24. On a legitimate debit or credit card, the information coded on the card's magnetic stripe will match the information embossed on the front of the card. This information includes the account number, expiration date, and cardholder's name, among other information. Whereas on a cloned card, the information coded on the magnetic stripe will not match the information embossed on the front of the card. For example, if a suspect re-encodes victim EBT card information onto a pre-existing gift card's magnetic stripe or a blank white plastic card with a magnetic stripe, the magnetic stripe will be coded with the EBT card information, but the card itself will still bear the information of the gift card or bear no information if it is a blank white plastic card.

25. Based on my training, experience, and participation in this investigation, I know that the victim card data harvested to clone cards is often obtained from what is colloquially referred to as "skimming activity."

26. The term "skimming" is used to describe activity that involves unlawfully obtaining debit and credit card information by using technological devices to surreptitiously record victim accountholder's debit and credit card numbers and personal identification numbers at, for example, ATMs or point-of-sale terminals. For example, individuals conducting ATM "skimming" may install a skimming device into the card reader of the ATM to record the debit or credit card numbers, as well as a camera or keypad overlay on the ATM keypad to record the associated PIN number. Those individuals will then return to the ATM to

collect the card number and PIN information stored on the installed device.

27. As described above, suspects then manufacture cloned and fraudulent debit or credit cards that bear the victim accountholder's account information that was obtained from skimming. Once that information is loaded onto another fraudulent card (e.g., a gift card or blank plastic card), members of the scheme then use that fraudulent card to withdraw cash from the victim accountholder's bank accounts or to make purchases with the victim accountholder's account.

28. In or about September 2022, local law enforcement conducted a surveillance and arrest operation in the Los Angeles, California area. This operation was planned in response to the large number of unauthorized withdrawals occurring at ATMs in the Los Angeles area during a short period of time. Specifically, law enforcement had analyzed fraudulent EBT withdrawal data and noticed a high volume of unauthorized withdrawals on specific dates and times that coincided with the dates when the majority of benefits are disbursed to EBT cardholders.

29. As a result of this operation, local law enforcement established surveillance at select ATMs that were used to conduct a significant volume of EBT fraud. Law enforcement surveilled those ATMs around the dates when benefits had been disbursed, observed suspects that withdrew a high volume of unauthorized withdrawals and that conducted those withdrawals in rapid succession, and arrested multiple individuals believed to

be making fraudulent withdrawals of EBT benefits. As a result, law enforcement arrested approximately 16 suspects. All of the arrested suspects were later determined to be citizens of countries other than the United States who did not have documentation to be lawfully present in the United States. All of the individuals arrested were released from local custody within hours of their arrest and absconded from any future judicial proceedings.

30. In or about February 2023, in response to a further increase in unauthorized cash withdrawals utilizing EBT cards after the local law enforcement September 2022 operation, federal law enforcement conducted a similar surveillance and arrest operation in the Los Angeles, California area. Law enforcement established surveillance around the dates when benefits had been disbursed at select high-volume EBT fraud ATMs. Law enforcement arrested three suspects that withdrew a high volume of unauthorized withdrawals and that conducted those withdrawals in rapid succession. Two of those defendants came to the ATM together, possessed 35 cloned EBT cards at the time of arrest, and later analysis of historic ATM surveillance data showed that they had made more than $190,000 in past attempted fraudulent EBT withdrawals from a single bank since October 2022. One additional defendant possessed 269 cloned EBT cards at the time of arrest, and later analysis of historic ATM surveillance data showed that the defendant had made more than $70,000 in past attempted fraudulent EBT withdrawals from a single bank since January 2023. All three of these defendants

were determined to be citizens of Romania, who did not have documentation to be lawfully present in the United States. The three arrested defendants were ordered detained pending trial by the Hon. Karen Stevenson and Hon. Margo A. Rocconi. A federal grand jury returned two indictments against the three defendants for bank fraud, in violation of 18 U.S.C. § 1344; aggravated identity theft, in violation of 18 U.S.C. § 1028A; use of unauthorized access devices, in violation 18 U.S.C. § 1029(a)(2); and possession of unauthorized access devices, in violation of 18 U.S.C. § 1029(a)(3), in 23-CR-0076-FLA and 23-CR-0077-JFW.

31. In or about March 2023, federal law enforcement conducted another surveillance and arrest operation in the Los Angeles, California area. Law enforcement established surveillance around the dates when benefits had been disbursed at select high-volume EBT fraud ATMs. Law enforcement arrested eleven suspects that conducted a high volume of unauthorized transactions and that conducted those transactions in rapid succession. At the time of their arrest, the suspects had in their possession over 400 cloned cards, $120,000 in illicitly obtained funds, and multiple skimming devices.

32. Ten out of the eleven of these defendants were determined to be citizens of Romania, who did not have documentation to be lawfully present in the United States.

B. Background of Current Operation to Combat EBT Fraud

33. Data provided by DSS, based in part upon reported fraud by victims, reported fraud to local law enforcement, bank

records, and surveillance indicates that as of in or about November 2023, there has been over $100 million in stolen funds from victim EBT cards.

34. Between in or about June 2023 and in or about November 2023, more than $45.3 million has been stolen from victim EBT cards. Of the approximately $45.3 million stolen, approximately $17.3 million has been stolen from victim EBT cards in Los Angeles County alone. The majority of these funds were stolen through unauthorized ATM withdrawals.

35. Between on or about November 1, 2023, and on or about November 5, 2023, more than $9.5 million was stolen from victim EBT cards largely through unauthorized ATM withdrawals. Of the approximately $9.5 million stolen from victim EBT cards in the beginning of January 2023, more than $2.7 million was stolen, almost entirely through unauthorized ATM withdrawals, in Los Angeles County alone.

36. For example, between on or about November 1, 2023, and on or about November 5, 2023, more than $129,000 was withdrawn from ATMs at a single financial institution branch located in Lancaster, California in Los Angeles County. The unauthorized withdrawals conducted during these five days and at this single bank branch affected approximately 143 victim EBT cardholders. The dates of these withdrawals coincided with the disbursement by DSS of EBT benefits, including CalFresh and CalWORKs.

37. Based upon my training and experience conducting access device fraud investigations, I know that suspects committing access device fraud schemes will often target

particular BINs when harvesting stolen card information collected from skimming devices. Thus, suspects using skimming may target the BIN associated with DSS, in essence, targeting CalFresh and CalWORKs benefits. Moreover, based upon my training and experience, the sheer volume of unauthorized ATM withdrawals occurring during the early days of the month is further indicative that suspects participating in the fraud scheme at issue are targeting EBT cards because benefits are typically disbursed to EBT cardholders during the early days of each month.

38. Law enforcement has also reviewed ATM surveillance provided by financial institutions that administer EBT accounts that relate to the fraud scheme at issue. During the unauthorized ATM withdrawals, suspects can often be seen holding stacks of cards and conducting withdrawals in quick succession at one ATM. Based upon my training and experience, I know that suspects perpetrating access device fraud schemes will often conduct unauthorized withdrawals using cloned cards in rapid succession at ATMs.

39. Based upon the rapid succession of unauthorized ATM withdrawals being conducted, the fact that the cards being used to conduct the unauthorized cash withdrawals are nearly all cloned EBT cards, and the fact that nearly all of the unauthorized withdrawals are happening during the early days of the month, I believe that suspects participating in the fraud scheme at issue are ostensibly targeting EBT cards.

C. SANDU and NECHITA Committed EBT Fraud Using Unauthorized Access Devices on February 1, 2024

40. Based upon the large dollar amount being stolen from victim EBT cards, the number of victims impacted, the concentration of unauthorized ATM withdrawals occurring in particular areas, and the large number of unauthorized ATM withdrawals occurring at singular bank locations, law enforcement conducted a surveillance and arrest operation in February 2024.

41. On February 1, 2024, law enforcement was conducting physical surveillance at various bank and ATM locations throughout Los Angeles County, including a U.S. Bank ATM terminal located at 18200 Western Avenue, Gardena ("18200 ATM"), which was identified as one of the top ATM locations in Los Angeles for EBT fraud. Based on DSS fraud data, surveillance was conducted beginning at approximately 5:00 a.m.

42. DSS reported to law enforcement that the CalFresh and CalWORKs benefits had been disbursed into the EBT accounts at approximately 6:00 a.m. on February 1, 2024.

43. During this surveillance, law enforcement observed an unknown individual, later identified as NECHITA, arrive at the 18200 ATM at 7:14 a.m. NECHITA was wearing a black sweatshirt, dark pants, and a black baseball cap. Law enforcement observed, and US Bank confirmed, that upon arriving at the 18200 ATM, NECHITA immediately placed something on the 18200 ATM surveillance camera in what appeared to be an attempt to conceal his actions and identity. Law enforcement observed, and US Bank

confirmed, NECHITA withdrew approximately $2,440 from the 18200 ATM in rapid succession using approximately four different access devices. One of these transactions comprised of a $740 withdrawal from the EBT account ending in 6935. At 7:18 a.m., law enforcement saw NECHITA leaving the 18200 ATM. Later on February 1, 2024, law enforcement interviewed victim G.J., the rightful owner of the EBT card ending in 6935, who stated that she did not give anyone permission to be in possession of her EBT card information, nor did she give anyone permission to utilize her EBT account information to withdraw money.

44. At 7:25 a.m., law enforcement saw SANDU at the walk-up 18200 ATM terminal. SANDU was wearing a black Under Armour sweatshirt and dark pants. Law enforcement observed, and US Bank confirmed, that SANDU withdrew approximately $1,640 in cash from the 18200 ATM in rapid succession using approximately three different access devices and used two additional access devices to conduct balance inquires that were unsuccessful. One of these transactions comprised of a $840 withdrawal from the EBT account ending in 4525.

45. At 7:30 a.m., law enforcement observed SANDU leave the 18200 ATM and walk across Western Avenue toward the Subject Vehicle. Law enforcement identified themselves as police and attempted to detain SANDU, but he did not listen to law enforcement commands and instead walked quickly towards the entrance of Ted's Liquor located at 18303 South Western Avenue, Gardena. Law enforcement observed SANDU attempt to hide something on the counter of the liquor store. Law enforcement

detained SANDU and found five access devices (later determined to be cloned cards) hidden on the counter. SANDU was arrested and found to be in possession of $1,640 in cash and of SUBJECT DEVICE 1.

46. Based on the date, time, ATM location, presence of multiple, and successive ATM withdrawals on multiple EBT cardholder accounts during a short time period, law enforcement detained NECHITA and SANDU in order to investigate further.

47. The five cloned cards SANDU attempted to discard on the counter of the liquor store consisted of a variety of re-encoded prepaid cards and gift cards. The cards also had stickers placed on them with what appeared to be, based on my training and experience, card balances and victim PINs.

48. Approximately 14 cloned EBT cards were located in the Subject Vehicle that NECHITA was getting into at the time he was detained. The cloned cards consisted of a variety of re-encoded prepaid cards and gift cards. The cards also had stickers placed on them with what appeared to be, based on my training and experience, card balances and victim PINs.

49. Law enforcement confirmed these were cloned EBT cards by reading the magnetic stripe and determined through United States Department of Agriculture Office of Inspector General that the cards belonged to other real individuals, not NECHITA or SANDU. Moreover, the cloned cards also were affixed with stickers bearing victim PIN numbers that corresponded to each cloned card and were needed in order to conduct the unauthorized ATM withdrawals.

50. SANDU also had approximately $1,640 in cash in his pants pocket, which was close in value to the approximately $1,640 in total unauthorized ATM withdrawals. US Bank ATM surveillance photographs obtained by law enforcement also clearly depicted NECHITA and SANDU at the ATM conducting the unauthorized withdrawals using cloned EBT cards and directly corroborated law enforcement's surveillance observations.

51. When asked to identify himself, NECHITA provided the name "Julio Zamora" and had an "International Driver's License" in the name "Julio Zamora" and birth date of February 7, 1981. Identification by Immigration and Customs Enforcement (ICE) of NECHITA is pending at this time. However, Romanian National Police provided identification documents of NECHITA as "Lucian Ionut Nechita."

52. Based on my review of domestic and foreign law enforcement database records, NECHITA was previously arrested in Romania for organized crime and trafficking of human beings in Romania in 2008 and was sentenced to 8 years in Romanian prison.

53. When asked to identify himself SANDU simply stated his name was "Sandu." A booking sheet from a DUI arrest several weeks ago was located in the vehicle and it listed SANDU's name as "Marian Sandu." This identification by Immigration and Customs Enforcement ("ICE") is pending at this time.

54. Based on my review of domestic and foreign law enforcement database records, SANDU has prior arrests in Romania, the United Kingdom, and a few weeks ago here in Los Angeles for driving under the influence of drugs and/or alcohol.

55. Based on my training and experience, I know that individuals conducting access device fraud schemes will often conceal their true identities by obtaining fictitious IDs to enter the country illegally while evading detection by law enforcement.

56. SUBJECT DEVICE 1 was retrieved from SANDU's pockets and SUBJECT DEVICE 2 was retrieved from NECHITA's person.

57. Both NECHITA and SANDU were arrested, read their Miranda warnings, and invoked their right to counsel.

58. Law enforcement ceased any questioning of NECHITA and SANDU after they indicated they would like to speak with a lawyer.

V. TRAINING AND EXPERIENCE REGARDING IDENTITY THEFT CRIMES

59. Based on my training and experience and information obtained from other law enforcement officers who investigate identity theft, I know the following:

a. It is common practice for individuals involved in identity theft, bank fraud, and access device fraud crimes to possess and use multiple digital devices at once. Such digital devices are often used to facilitate, conduct, and track fraudulent transactions and identity theft. Suspects often use digital devices to perpetrate their crimes due to the relative anonymity gained by conducting financial transactions electronically or over the internet. They often employ digital devices for the purposes, among others, of: (1) applying online for fraudulent credit cards; (2) obtaining or storing personal identification information for the purpose of establishing or

modifying fraudulent bank accounts and/or credit card accounts; (3) using fraudulently obtained bank accounts and/or credit card accounts to make purchases, sometimes of further personal information; (4) keeping records of their crimes; (5) researching personal information, such as social security numbers and dates of birth, for potential identity theft victims; and (6) verifying the status of stolen access devices.

b. Oftentimes identity thieves take pictures of items reflecting their stolen identities, including items retrieved from stolen mail or mail matter, with their cellphones.

c. It is also common for identity thieves to keep "profiles" of victims on digital devices. Such "profiles" contain the personal identifying information of victims, such as names, Social Security numbers, dates of birth, driver's license or state identification numbers, alien registration numbers, passport numbers, and employer or taxpayer identification numbers. Identity thieves often keep such information in their cars, storage units, and in their digital devices.

d. It is common for identity thieves, and individuals engaged in bank fraud, access device fraud, and identification document fraud to use equipment and software to print credit and identification cards, to create magnetic strips for credit cards, to use embossing machines to create credit cards, to use laser printers to create checks, and to use magnetic card readers to read and re-encode credit cards. These types of devices are routinely kept where the person will have

easy access to such devices, such as on their person or in their cars or homes or storage units. Software relevant to such schemes can also often be found on digital devices, such as computers.

e. Based on my training and experience, I know that individuals who participate in identity theft, bank fraud, and access device fraud schemes often have co-conspirators, and often maintain telephone numbers, email addresses, and other contact information and communications involving their co-conspirators in order to conduct their business. Oftentimes, they do so on their digital devices. Suspects often use their digital devices to communicate with co-conspirators by phone, text, email, and social media, including sending photos. Suspects may also have paper copies of such records, which they may keep on their person or in their cars, homes, or storage units.

f. Individuals engaged in mail and identity theft often use multiple digital devices, which they may keep on their person or in their cars or homes.

VI. TRAINING AND EXPERIENCE ON DIGITAL DEVICES[2]

60. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I

---

[2] As used herein, the term "digital device" includes the SUBJECT DEVICES as well as any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as paging devices, mobile telephones, and smart phones; digital cameras; gaming consoles; peripheral

(footnote cont'd on next page)

know that the following electronic evidence, inter alia, is often retrievable from digital devices:

a. Forensic methods may uncover electronic files or remnants of such files months or even years after the files have been downloaded, deleted, or viewed via the Internet. Normally, when a person deletes a file on a computer, the data contained in the file does not disappear; rather, the data remain on the hard drive until overwritten by new data, which may only occur after a long period of time. Similarly, files viewed on the Internet are often automatically downloaded into a temporary directory or cache that are only overwritten as they are replaced with more recently downloaded or viewed content and may also be recoverable months or years later.

b. Digital devices often contain electronic evidence related to a crime, the device's user, or the existence of evidence in other locations, such as, how the device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials on the device. That evidence is often stored in logs and other artifacts that are not kept in places where the user stores files, and in places where the user may be unaware of them. For example, recoverable data can include evidence of deleted or edited files; recently used tasks and processes; online nicknames and passwords in the

---

input/output devices, such as keyboards, printers, scanners, monitors, and drives; related communications devices, such as modems, routers, cables, and connections; storage media; and security devices.

form of configuration data stored by browser, e-mail, and chat programs; attachment of other devices; times the device was in use; and file creation dates and sequence.

c. The absence of data on a digital device may be evidence of how the device was used, what it was used for, and who used it. For example, showing the absence of certain software on a device may be necessary to rebut a claim that the device was being controlled remotely by such software.

d. Digital device users can also attempt to conceal data by using encryption, steganography, or by using misleading filenames and extensions. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Law enforcement continuously develops and acquires new methods of decryption, even for devices or data that cannot currently be decrypted.

61. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that it is not always possible to search devices for data during a search of the premises for a number of reasons, including the following:

a. Digital data are particularly vulnerable to inadvertent or intentional modification or destruction. Thus, often a controlled environment with specially trained personnel may be necessary to maintain the integrity of and to conduct a complete and accurate analysis of data on digital devices, which may take substantial time, particularly as to the categories of electronic evidence referenced above. Also, there are now so

many types of digital devices and programs that it is difficult to bring to a search site all of the specialized manuals, equipment, and personnel that may be required.

b. Digital devices capable of storing multiple gigabytes are now commonplace. As an example of the amount of data this equates to, one gigabyte can store close to 19,000 average file size (300kb) Word documents, or 614 photos with an average size of 1.5MB.

62. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

VII. CONCLUSION

63. For all of the reasons described above, there is probable cause to believe that NECHITA and SANDU have committed a violation of 18 U.S.C. § 1029(a)(2) (use of unauthorized access devices). There is also probable cause that the items to be seized described in Attachment B will be found in a search of the SUBJECT DEVICES as described in Attachment A.

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on this 2nd day of February, 2024.

THE HONORABLE JACQUELINE CHOOLJIAN
UNITED STATES MAGISTRATE JUDGE